ANS-C01 Q&As

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ans-c01.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company operates its IT services through a multi-site hybrid infrastructure. The company deploys resources on AWS in the us-east-1 Regionand in the eu-west-2 Region. The company also deploys resources in its own data centers that are located in the United States (US) and in theUnited Kingdom (UK). In both AWS Regions, the company uses a transit gateway to connect 15 VPCs to each other. The company has createda transit gateway peering connection between the two transit gateways. The VPC CIDR blocks do not overlap with each other or with IPaddresses used within the data centers. The VPC CIDR prefixes can also be aggregated either on a Regional level or for the company\\'s entireAWS environment.The data centers are connected to each other by a private WAN connection. IP routing information is exchanged dynamically through InteriorBGP (iBGP) sessions. The data centers maintain connectivity to AWS through one AWS Direct Connect connection in the US and one DirectConnect connection in the UK. Each Direct Connect connection is terminated on a Direct Connect gateway and is associated with a localtransit gateway through a transit VIF.Traffic follows the shortest geographical path from source to destination. For example, packets from the UK data center that are targeted toresources in eu-west-2 travel across the local Direct Connect connection. In cases of cross-Region data transfers, such as from the UK datacenter to VPCs in us-east-1, the private WAN connection must be used to minimize costs on AWS. A network engineer has configured eachtransit gateway association on the Direct Connect gateway to advertise VPC-specific CIDR IP prefixes only from the local Region. The routestoward the other Region must be learned through BGP from the routers in the other data center in the original, non-aggregated form.The company recently experienced a problem with cross-Region data transfers because of issues with its private WAN connection. Thenetwork engineer needs to modify the routing setup to prevent similar interruptions in the future. The solution cannot modify the originaltraffic routing goal when the network is operating normally.Which modifications will meet these requirements? (Choose two.)

A. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add the company\\'sentire AWS environment aggregate route to the list of subnets advertised through the local Direct Connect connection.

B. Add the CIDR prefixes from the other Region VPCs and the local VPC CIDR blocks to the list of subnets advertised through the localDirect Connect connection. Configure data center routers to make routing decisions based on the BGP communities received.

C. Add the aggregate IP prefix for the other Region and the local VPC CIDR blocks to the list of subnets advertised through the local DirectConnect connection.

D. Add the aggregate IP prefix for the company\\'s entire AWS environment and the local VPC CIDR blocks to the list of subnets advertisedthrough the local Direct Connect connection.

E. Remove all the VPC CIDR prefixes from the list of subnets advertised through the local Direct Connect connection. Add both Regionalaggregate IP prefixes to the list of subnets advertised through the Direct Connect connection on both sides of the network. Configure datacenter routers to make routing decisions based on the BGP communities received.

Correct Answer: CE

If the private WAN failed, the network engineer would swing the traffic to the other region through the local Direct Connect and the Transit Gateways. That is the requirement. The solution is that the local DC has 2 kinds of route to the other

region VPCs. One is the existing CIDR-based routes via the private WAN, another is the advertised aggregated routes from the local Direct Connect connection. CIDR-based routes are prior to the aggregated routes advertised from Direct

Connect connection due to the longest prefix match routing algorithm.

The options which match this solution are C and E.

QUESTION 2

A company has an AWS account with four VPCs in the us-east-1 Region. The VPCs consist of a development VPC and three production VPCsthat host various workloads.The company has extended its on-premises data center to AWS with AWS Direct Connect by using a Direct Connect gateway. The company nowwants to establish connectivity to its production VPCs and development VPC from on premises. The production VPCs are allowed to routedata to each other. However, the development VPC must be isolated from the production VPCs. No data can flow between the developmentVPC and the production VPCs.In preparation to implement this solution, a network engineer creates a transit gateway with a single transit gateway route table. Defaultroute table association and default route table propagation are turned off. The network engineer attaches the production VPCs, thedevelopment VPC, and the Direct Connect gateway to the transit gateway. For each VPC route table, the network engineer adds a route to0.0.0.0/0 with the transit gateway as the next destination.Which combination of steps should the network engineer take next to complete this solution? (Choose three.)

A. Associate the production VPC attachments with the existing transit gateway route table. Propagate the routes from these attachments.

B. Associate all the attachments with the existing transit gateway route table. Propagate the routes from these attachments.

C. Associate the Direct Connect gateway attachment with the existing transit gateway route table. Propagate the Direct Connect gatewayattachment to this route table.

D. Change the security group inbound rules on the existing transit gateway network interfaces in the development VPC to allowconnections to and from the on-premises CIDR range only.

E. Create a new transit gateway route table. Associate the new route table with the development VPC attachment. Propagate the DirectConnect gateway and development VPC attachment to the new route table.

F. Create a new transit gateway with default route table association and default route table propagation turned on. Attach the DirectConnect gateway and development VPC to the new transit gateway.

Correct Answer: ACE

ACE are correct - Options B, D, and F don\\'t adhere to the provided requirements. Option B would not provide the required isolation for the development VPC. Option D won\\'t be effective as the restriction should be on the routing level, not on the security group level. Option F would create unnecessary complexity and potential overlap in connectivity.

QUESTION 3

A company has set up hybrid connectivity between its VPCs and its on-premises data center. The company has the on-premises.example.comsubdomain configured at its DNS server in the on-premises data center. The company is using the aws.example.com subdomain for workloadsthat run on AWS across different VPCs and accounts. Resources in both environments can access each other by using IP addresses. Thecompany wants workloads in the VPCs to be able to access resources on premises by using the on-premises.example.com DNS names.Which solution will meet these requirements with MINIMUM management of resources?

A. Create an Amazon Route 53 Resolver outbound endpoint. Configure a Resolver rule that conditionally forwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs.

B. Create an Amazon Route 53 Resolver inbound endpoint and a Resolver outbound endpoint. Configure a Resolver rule that conditionallyforwards DNS queries for on-premises.example.com to the on-premises DNS server. Associate the rule with the VPCs.

C. Launch an Amazon EC2 instance. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance\\'s IP address as a custom DNS server in each VPC.

D. Launch an Amazon EC2 instance in each VPC. Install and configure BIND software to conditionally forward DNS queries for on-premises.example.com to the on-premises DNS server. Configure the EC2 instance\\'s IP address as a custom DNS server in each VPC.

Correct Answer: A

we need an outbound endpoint because we want to resolve it with an on-premises DNS query

QUESTION 4

A retail company is running its service on AWS. The company\\'s architecture includes Application Load Balancers (ALBs) in public subnets. TheALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can callexternally hosted services over the internet by using a NAT gateway.The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source ofthis increased usage.Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

A. Enable VPC flow logs on the NAT gateway\\'s elastic network interface. Publish the logs to a log group in Amazon CloudWatch Logs. UseCloudWatch Logs Insights to query and analyze the logs.

B. Enable NAT gateway access logs. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to queryand analyze the logs.

C. Configure Traffic Mirroring on the NAT gateway\\'s elastic network interface. Send the traffic to an additional EC2 instance. Use tools suchas tcpdump and Wireshark to query and analyze the mirrored traffic.

D. Enable VPC flow logs on the NAT gateway\\'s elastic network interface. Publish the logs to an Amazon S3 bucket. Create a custom tablefor the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

E. Enable NAT gateway access logs. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athenato describe the log structure. Use Athena to query and analyze the logs.

Correct Answer: AD

A. Yes, this would work.

B. Not a real thing, wrong

C. We don\\'t need to do packet inspection to analyze costs. This won\\'t help with costs at all.

D. The most obvious right answer.

E. Like B, not a real thing.

QUESTION 5

A development team is building a new web application in the AWS Cloud. The main company domain, example.com, is currently hosted in anAmazon Route 53 public hosted zone in one of the company\\'s production AWS accounts.The

developers want to test the web application in the company\\'s staging AWS account by using publicly resolvable subdomains under theexample.com domain with the ability to create and delete DNS records as needed. Developers have full access to Route 53 hosted zoneswithin the staging account, but they are prohibited from accessing resources in any of the production AWS accounts.Which combination of steps should a network engineer take to allow the developers to create records under the example com domain?(Choose two.)

A. Create a public hosted zone for example com in the staging account

B. Create a staging example.com NS record in the example.com domain. Populate the value with the name servers from thestaging.example.com domain. Set the routing policy type to simple routing.

C. Create a private hosted zone for staging example com in the staging account.

D. Create an example com NS record in the staging example.com domain. Populate the value with the name servers from theexample.com domain. Set the routing policy type to simple routing.

E. Create a public hosted zone for staging.example.com in the staging account.

Correct Answer: BE

When a client queries a DNS server for a domain name, the DNS server typically starts by looking for NS records to determine which name servers are authoritative for the domain. The DNS server then queries the authoritative name servers to obtain the information about the domain that the client requested.

For example, suppose you own the domain example.com, but you want to delegate control of the subdomain sub.example.com to a different set of name servers. You would create NS records in the example.com zone file that point to the name servers for sub.example.com. This tells DNS servers that the name servers for sub.example.com are authoritative for that subdomain, and they should query those name servers for any requests related to sub.example.com.